Securing connectivity between organizations presents unique challenges to application providers.

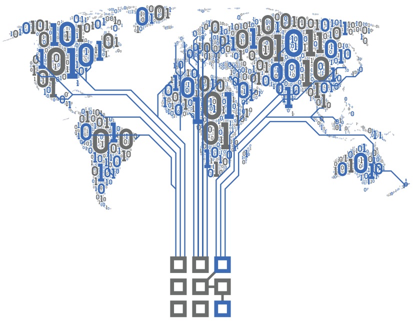
Legacy WAN infrastructure is difficult and expensive to manage. When connectivity spans hundreds of unique organizations the problems become nearly insurmountable, requiring dedicated teams of network engineers and security specialists.

Connectivity solutions such as Data Mesh integrate security and compliance features in ways that are not possible in legacy solutions, while improving efficiency in network infrastructure deployment and lifecycle management.

AUTHENTICATION

Pre-shared keys (PSK) are the most common method for authenticated VPN connectivity and present significant risk when not implemented properly. Certificate-based authentication is much more secure, but is difficult to implement and traditionally requires advanced skill sets.

Trustgrid provides the ‘root of trust’ in a Public Key Infrastructure (PKI) built by our security experts to enable automated certificate deployment and lifecycle management across all Trustgrid connections.



- Upon installation, devices enroll into the Trustgrid PKI and are issued certificates that are managed centrally from the Trustgrid cloud Certificate Authority (CA).
- Certificates are issued per device and are subsequently used to uniquely identify and authenticate devices before allowing them to receive or send network traffic on a Trustgrid network.

As an additional layer of security, Trustgrid takes advantage of hardware security technology on devices where it's available. This hardware-level device attestation provides a kind of "dual factor" authentication for devices connecting onto a Trustgrid network, which allows devices to cryptographically verify that peers are running on registered hardware.

AUTHORIZATION

Implementing secure network access and authorization policies is traditionally a difficult task that requires expert knowledge to implement and maintain. Lack of sufficient network security process and personal often leads to cutting corners.

Central to the security of the Trustgrid's Data Mesh Platform is an authorization model derived from Google's Beyond Corp (aka Zero Trust from Forrester) initiative.

This model places an implicit deny on all traffic and furthermore cannot be configured to allow all traffic. Many breaches have been caused because of "allow everything" network policies that were put in place to bypass the burden of proper security configuration.

- Trustgrid uses a security model based on "authorization domains" to allow a user to easily describe which network devices are allowed to peer in any given Trustgrid mesh network.
- Through Trustgrid's cloud portal or via API, the user can then centrally define the external systems and traffic types that are allowed on the network in an intuitive fashion.
- By restricting all access that hasn't been explicitly allowed, the user can always be sure that their network policies are as secure as possible.

In addition to providing an easy to use and intuitive way to give required access to devices and systems in the Data Mesh, the platform provides mechanisms for quickly revoking authorization in situations such as a potential breach.

With a single click of a button, connected devices can be instantly removed from the network until the situation is investigated, while maintaining the device configuration for when it is ready to be added back onto the network.

AUDITING

Monitoring important events on a large network with many locations is a difficult task. Software updates, configuration changes, and potential security incidents must often be tracked for compliance and are necessary for a coherent incident response process.

These kinds of auditable events must often be gathered by different means in different places, and then stored and reported on from an expensive external reporting tool. Properly implementing a cohesive auditing policy not only often requires significant capital investment, but is operationally expensive to deploy, maintain and monitor.

Trustgrid provides innovative and easy to use auditing capabilities that make auditing network infrastructure a painless process. All software updates and configuration changes are audited to the Trustgrid central log repository where they can be viewed in the Trustgrid portal or exported to object storage such as AWS S3.

Notifications such as email or SMS can also be triggered by change events to ensure prompt visibility and response to unauthorized system activity.

In addition to auditing system changes, the user can optionally define a policy that requires 3rd party signoff for pending changes before they can occur. This advanced change control feature provides an extra layer of insurance when required for compliance or insisted upon by advanced security policies.

SECURE DATA PATH

Traditional site-to-site VPN connectivity relies on the IPSec protocol. This often requires complex configuration and suffers from problems of exposing too much of the remote and local network, as well as being very cumbersome to configure when the local and remote locations use overlapping IP spaces.

All data on a Trustgrid network is private, encrypted and tunneled from between locations using mutually-authenticated Transport Layer Security (TLS), which the Internet Engineering Task Force (IETF) recommends as a replacement to IPSec VPN technology.

- Behind the scenes Trustgrid ensures that these connections are using best of breed encryption to ensure that customer data is always safe.
- In addition, customers can optionally use their own external PKI and certificates, if required by security policy, such that the encryption being used to tunnel customer data across the network is not dependent on Trustgrid’s PKI whatsoever.

Though Trustgrid’s device control plane runs on secure multi-tenant cloud infrastructure, the customer’s private data path only runs on infrastructure owned by the customer. This ensures that the customer’s private data only exists on their own systems and is not flowing through centralized, multi-tenant gateways that touch hundreds of vendors’ connections concurrently.

AUTOMATED SOFTWARE MANAGEMENT

A significant difficulty in securing traditional VPNs is the application of patches and updates to connected hardware appliances.

Trustgrid customers often own and maintain hundreds or thousands of these devices and struggle to efficiently patch them. This leaves significant security and compliance vulnerabilities unaddressed in customer and vendor datacenters.

Trustgrid devices are always ensured to be running the latest software versions and patches for operation. Software updates are seamlessly applied during the customer assigned maintenance window and can optionally require explicit signoff before an update is applied. This approach ensures that software updates occur in a timely manner and only when expected, while also taking care to not to affect customer traffic in an adverse way while being applied.

> Because Trustgrid is software defined and running on non-proprietary hardware, end of life and device obsolescence are no longer an issue.

EVOLVE WITH TRUSTGRID

Ensuring the security of legacy connectivity solutions is a manual and time-consuming task that introduces substantial risk, especially when deployed at enterprise scale.

Trustgrid's Data Mesh Platform natively implements modern security models and automates much of the security burden placed on product and IT teams. By combining secure software-defined networking, management and automation tools, Trustgrid solutions provide feature-rich and future proof connectivity that allows software providers to focus on software, not IT infrastructure.

888.308.8995
info@trustgrid.io